

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-148697

(43)Date of publication of application : 29.05.2001

(51)Int.Cl.

H04L 9/32

G06F 12/14

G09C 1/00

H04L 9/10

(21)Application number : 2000-262692

(71)Applicant : COMPAQ COMPUTER CORP

(22)Date of filing : 31.08.2000

(72)Inventor : HOPKINS DALE WEBSTER

MCKAY MICHAEL

LANGFORD SUSAN

HINES LARRY

(30)Priority

Priority number : 1999 389157

Priority date : 02.09.1999

Priority country : US

(54) METHOD FOR COMMUNICATING INFORMATION VIA CHANNEL HAVING LOW RELIABILITY

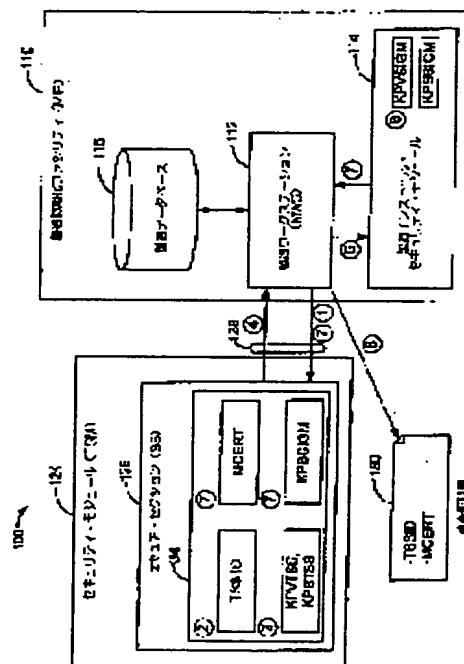
(57)Abstract:

PROBLEM TO BE SOLVED: To attain the communication security between the devices which are connected to a network.

SOLUTION: A secure section SS 126 of a security module TSM 124 included in a device stores the serial numbers SSID sent from a manufacturing initialization facility MIF 110 via a network into a storage 34 ((2)) and then generates and stores a public key pair ((3)). The public key pair includes a secret part KPVS and a public part KPBSS and transmits only the part KPBSS to the facility MIF 110 ((4)). A manufacturing install security module MISM 114 generates and stores a manufacturer certificate including the part KPBSS and a secret signature key KPVSIGM ((6)), and also the certificate is transmitted to the section SS 126 of the module TSM 124 and stored there together with a public signature key KPBSIGM of the facility MIF 110 ((7)). The facility MIF 110 also generates an inspection certificate 130.

The internal secrecy is stored in every device and

certificate and accordingly the devices can authenticate and safely communicate with each other even via a channel having low reliability without being previously programmed by means of the secrecy of an operator.



LEGAL STATUS

[Date of request for examination]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2001-148697
(P2001-148697A)

(43) 公開日 平成13年5月29日 (2001.5.29)

(51) Int.Cl. ⁷	識別記号	F I	テマコード [*] (参考)
H 0 4 L 9/32		G 0 6 F 12/14	3 2 0 B
G 0 6 F 12/14	3 2 0	G 0 9 C 1/00	6 6 0 B
G 0 9 C 1/00	6 6 0	H 0 4 L 9/00	6 7 5 B
H 0 4 L 9/10			6 2 1 A

審査請求 未請求 請求項の数11 O L (全 16 頁)

(21) 出願番号 特願2000-262692(P2000-262692)

(22) 出願日 平成12年8月31日 (2000.8.31)

(31) 優先権主張番号 09/389157

(32) 優先日 平成11年9月2日 (1999.9.2)

(33) 優先権主張国 米国 (U S)

(71) 出願人 591030868
コンパック・コンピューター・コーポレーション
COMPAQ COMPUTER CORPORATION
アメリカ合衆国テキサス州77070, ヒューストン, ステイト・ハイウェイ 249, 20555

(72) 発明者 デイル・ウェブスター・ホブキンス
アメリカ合衆国カリフォルニア州, サン・ホセ, ザンカー・ロード 2304

(74) 代理人 100089705
弁理士 社本 一夫 (外5名)

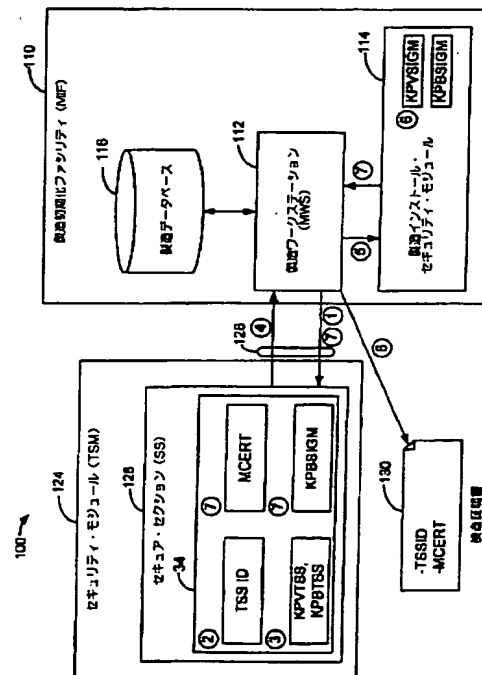
最終頁に続く

(54) 【発明の名称】 低信頼性のチャネルを介して情報を通信する方法

(57) 【要約】

【課題】 ネットワークに接続されるデバイス間の通信セキュリティを確立する。

【解決手段】 デバイス内の TSM124 の SS126 は、MIF110 からネットワークを介して送られた通し番号 SSID を記憶装置 34 に記憶し (②)、公開キー・ペアを生成し格納する (③)。該ペアは秘密部分 KPVS と公開部分 KPBSS を備え、公開部分のみを MIF に送信する (④)。MISM114 は、該公開部分及び秘密署名キー KPVSIGM を有する製造業者証明書を作成し、記憶する (⑥) とともに、TSM124 の SS126 に送信され、MIF の公開署名キー KPBSSIGM とともに記憶される (⑦)。MIF110 は、検査証明書 130 も生成する。内部機密が各デバイス及び証明書内に保持されるので、デバイスは、オペレータの機密を用いて予めプログラムされる必要無く、低信頼性のチャネルを介してでも、相互認証して安全に通信することができる。



【特許請求の範囲】

【請求項1】 オペレータに作用する他のデバイスと通信するための、該オペレータによって使用されるデバイスを製造する方法であって、製造業者は該製造業者及びその認可されたエージェント以外の他人にとって通常は入手不可能である製造業者キーを有し、通信が盗聴又はメッセージ変更から安全であることが保証されていない信頼性の低いチャネルによって行われる、デバイス製造方法において、

オペレータに関する機密を含む必要がなくかつ変形不可能境界内に含まれる回路としてのセキュア・セクションを含むように、デバイスを製造するステップと、製造されたデバイスに特定のデバイス識別子を用いてデバイスを初期化する初期化ステップと、セキュア・セクションをトリガして、内部機密を生成するステップと、セキュア・セクション内に、内部機密の非可逆性の暗号化変換を作成するステップと、デバイスから、非可逆性の暗号化変換を内部機密の公開部分として出力するステップと、製造業者キーを使用して、該公開部分及びデバイス識別子のデジタル署名を生成するステップとを含むことを特徴とする方法。

【請求項2】 請求項1記載の方法において、各デバイスは、特定のオペレータ又は該デバイスが接続されるネットワークに限定されていない、一般的なデバイスとして製造されていることを特徴とする方法。

【請求項3】 請求項1記載の方法において、該方法は更に、デバイスが適切に製造されたことを認証するためのステップを含むことを特徴とする方法。

【請求項4】 請求項1記載の方法において、非可逆性の暗号化変換を作成するステップは公開キーのペアを生成するステップを含み、該公開キーのペアの公開キー部分が内部機密の公開部分となることを特徴とする方法。

【請求項5】 公開部分と製造業者キーを用いる一意のデバイス識別子とのデジタル署名が存在する内部機密を有するデバイスを使用して、信頼性の無いチャネル環境において、デバイスとキー・サーバとの間に安全チャネルをセットアップする方法において、

デバイスに対してキー・サーバを認証する第1の認証ステップと、

内部機密を知っているデバイスのみが生成することができる応答を提供するようデバイスに要求することにより、キー・サーバに対して該デバイスを認証する第2の認証ステップと、

第1及び第2の認証ステップにおいてキー・サーバ及びデバイスによって提供された情報を用いて、キー・サーバ及びデバイスによって共有される共有機密を作成するステップと、

チャネルを介しての安全な通信のために、共有機密を使

用するステップとを含むことを特徴とする方法。

【請求項6】 請求項5記載の方法において、共有機密を使用するステップは、キー・サーバとデバイスとの間でデータを転送すること、キー・サーバとデバイスとの間でキーを転送すること、デバイスにおいてコンフィギュレーション値をセットすること、及び、デバイスからコンフィギュレーション値を読み出すことの少なくとも1つを含むことを特徴とする方法。

【請求項7】 ターゲット・デバイスとキー・サーバとの間で信頼性の低いチャネルを介してキー・サーバからターゲット・デバイスにキーをロードする方法であって、該ターゲット・デバイスの初期コンテンツが、信頼性の無いエンティティによって決定可能であると推定される、キー・ロード方法において、ターゲット・デバイスの安全な回路内で、予め値を決定することができない少なくとも1つの変数の関数であるセッション・キーを生成するステップと、信頼性の無いチャネル上に保護されたチャネルを構成する際に、セッション・キーを使用するステップと、保護されたチャネルを用いて、キー・サーバからターゲット・デバイスに少なくとも1つのキーをロードするステップとを含むことを特徴とする方法。

【請求項8】 請求項7記載の方法において、ターゲット・デバイスは、安全なネットワークに付加されるべき新たに製造された端末であり、機密を有していないと推定されることを特徴とする方法。

【請求項9】 信頼性の無いチャネルを介してキー・サーバからターゲット・デバイスに安全にキーをロードするシステムにおいて、

ターゲット・デバイス内に設けられ、(a)乱数発生器と、(b)指数演算器と、(c)乱数発生器と指数演算器の出力に基づいて、機密セッション・キーがロジック装置に関する知識及びその製造された状態とからは容易に生成することができないように、機密セッション・キーを生成するロジック装置とを備えたセキュア・チップと、

キー・サーバ内に設けられ、機密セッション・キーで符号化された該ターゲット・デバイスによって受信されるメッセージを解読し、該解読されたメッセージを用いて信頼性の無いチャネルを介してセキュア・チャネルを起動するキー・サーバ・ロジック装置とを具備することを特徴とするシステム。

【請求項10】 信頼性の低いチャネルを介して初期化キーでセキュリティ・デバイスを初期化する方法において、

機密であることが知られていないハードウェア構成のセキュリティ・デバイスの保護された部分内に機密を生成するステップと、

生成された機密を用いて、セキュリティ・デバイスと外部ノードとの間で安全に通信するステップとを含むこと

を特徴とする方法。

【請求項 11】 請求項 10 記載の方法において、外部ノードは、キー・サーバに関連付けられたノードであり、該方法はさらに、生成された機密キーを用いて確立された安全な通信チャネルを介して、キー・サーバからセキュリティ・デバイスに少なくとも 1 つのキーをロードするステップを含むことを特徴とする方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、暗号化システムに関し、特に、安全な (secure) 初期化を必要とする暗号化システムに関する。

【0002】

【従来の技術】 通信及びデータ記憶デバイスを好ましくないアクセス及び改変 (改竄) から保護するために、暗号化が使用されている。安全な通信には、いくつかの特徴がある。安全な通信の 1 つの特徴は、保護されたメッセージが、メッセージ送信側とメッセージ受信側以外のエンティティによっては読取ることができない、ということである。安全な通信の他の特徴は、受信側にメッセージが変更されたことを検出されないように、アタッカが送信側から受信側に伝送中のメッセージを変更することができない、ということである。メッセージをその変更が検出可能な方法で変更したとしても、大した問題ではない。すなわち、受信側が、変更されたメッセージを明らかな偽造又は通信エラーであるものとして、単純に破棄することができるためである。

【0003】 当然のことながら、実現可能な安全な通信により、十分な時間、労力及びコンピュータの能力があれば、メッセージを読出し可能又は変更可能にすることができる。このような能力があっても、アタッカが、メッセージに対する解読キーを有するか、又は、メッセージを「クラッキング」してその内容を読出すか又は変更されたメッセージを作成して、時間又は計算能力をその許容閾値を超えて消費するかしなければ、メッセージを読出すか又は変更することができない場合、メッセージは、読出し不可能か又は変更不可能であると推定される。一般に、安全な通信システムは、時間の閾値が、メッセージが機密であり続ける必要がある時間の長さより長いように設計されており、計算能力の閾値は、アタッカがメッセージをクラッキングすることによって取得する利益に見合ったコストであらゆる予測されたアタッカに入手可能な計算能力より、大幅に大きい。

【0004】 より一般的に述べると、暗号化システムは、該暗号化システムによって保護される通信又はデータ記憶システムの使用を制限するために採用される 1 つ又は複数の機密を保持するシステムである。なお、本明細書において、「通信システム」とは、伝統的に通信システムとして考えられなかったシステムを含んでおり、あるソース (すなわち送信元) からあるデスティネーシ

ョン (すなわち送信先) にデータを通信する場合、又は、安全な方法でデータをデータ記憶デバイス間で転送する (すなわち、データの書き手側からデータの読み手側への「通信」を安全にする) 場合の、あらゆるシステムを意味している。

【0005】 1 つ又は複数のメッセージを機密保護する際に、一般的な暗号化システムは、メッセージを機密のままにし、またメッセージの認証、完全性、及び非支払拒否性を確実にするために、使用される。当然のことながら、暗号化システムによっては、それら機能をすべて行うとは限らない。例えば、あるものは、文書を認証するためのシステムをセットアップするが、該認証された文書は、すべての視聴者が見れるようにオープンにされる。認証により、受信側は、メッセージの送信側と称している送信側が実際の送信側であるか否かを検査することができ、完全性により、受信側は、受信したメッセージがまさに送信されたメッセージであるか否かを検査することができ、非支払拒否性により、受信側は、メッセージが送信側によって実際に送信されたということを、送信側及びその他に証明することができる。

【0006】 通信システムの設計によっては、センシティブな暗号化オペレーションを厳密に制御することができるように、暗号システム・モジュールにおいて、暗号化機能が他の機能から分離されている。一般的な暗号システム・モジュールは、メッセージを暗号化し、解読し、照合するために使用するための機密を保持する。これら機密は、しばしば「キー」と呼ばれる。キーは、記憶されたデータを保護するか、通信チャネルを保護するか、又は、他の同様のタスクを保護するために使用することができる。データ又は通信チャネルを保護することにより、そのデータ又はチャネルの使用を、アクセスを保護するために使用されるキーを知っている人々又はエンティティのみに限定することができる。

【0007】 通信チャネルを保護する際のキーの使用法には、いくつもの方法がある。1 つの使用法は、メッセージの暗号化/解読に関係するものである。この使用法において、ソースからデスティネーションに通信するために使用されるチャネルは、必ずしも安全ではないと考えられる。安全でないチャネルは、アタッカがソースからデスティネーションに移動するトラフィックを盗聴する、「盗聴 (eavesdropping)」アタックに晒されやすい。また、安全でないチャネルは、アタッカがトラフィック内を盗聴する能力を有するだけでなく、それがソースからデスティネーションに進む際にメッセージを変更することもできる、「マン・イン・ザ・ミドル (man-in-the-middle)」アタックにも晒され易い。信頼性の無いチャネルは、実際には安全である場合も安全でない場合も有り得るが、安全でないと推定されるチャネルである。信頼性の無いチャネルに対して設計されているセキュリティ・システム

は、チャネルがある観点で安全ではないと推定するが、該システムは、システム設計によって付加されたセキュリティ基準無しに安全となるチャネルを介する場合と同じ方法で動作することになる。

【0008】ソースからデスティネーションへのトラフィックを暗号化することにより、これらのアタックを受けてしまうことを、大幅に困難なものにすることができる。暗号化により、プレインテキスト（平文）・メッセージ（すなわち、メッセージを所有していれば誰でも読出し可能なメッセージ）が、キーを用いて、暗号文メッセージに変換される。そして、このキーを知らなければ、暗号文がプレインテキスト・メッセージに容易に戻すことができない。暗号化は、プレインテキスト・メッセージとキーとをプロセス入力とする暗号化プロセスを用いて行われる。好ましくは、メッセージのセキュリティは、暗号化プロセスの詳細を知らないアタックによるものではない。暗号化プロセスは全く周知であって、セキュリティがアタックに知られていないキーによってのみ提供される、という暗号化システムが、より好適である。

【0009】安全な通信の上述した各々の有用性は、ポイント・オブ・セール（POS）端末ネットワークに関して説明することができる。POS端末ネットワークにおけるPOS端末は、商店と顧客との間の販売を容易にするために使用される。このPOS端末ネットワークでは、顧客は、販売をカバーするべく、その顧客の銀行預金口座から商店の銀行預金口座に資金を振替るよう、顧客の銀行に許可する。取引は、商店のPOS端末と他のネットワーク・デバイスとの間で1つ又は複数のメッセージを通信することによって行われる。POS端末ネットワークの1つの目的は、通信を保護することであるため、盗聴者又は窃盗犯（一般に、多くの暗号化テキストにおいて「アタック」と呼ばれる）は、メッセージ・キーを知らなければ、メッセージ・トラフィックを読み出すことも不可能であり、また、検出されることなくデータを変更することもできない。

【0010】明らかなように、販売取引に関わる当事者は、メッセージ・トラフィックが安全な通信の上述した態様を有していることを望む。顧客は、自身の口座番号がアタックによって読出し不可能であるように、通信が機密であることが確実であるよう望む。銀行は、資金が顧客によって正式に認められた時にのみ引出されるように、通信が信頼できることが確実であることを望む。アタックが商店の口座番号をアタックの口座番号に置換えるようにメッセージを編集することができないように、メッセージの完全性が保証されている必要がある。また、顧客が買って帰った商品に対し銀行が商店に支払いを行ったが、その顧客が取引を拒否し自身の口座から取引を取り消したいという場合が生じないようにするため、非支払拒否は、顧客の銀行にとって重要である。

【0011】安全な通信のこれらの面は、銀行及び顧客がこれらの間の通信を保護するステップをとる場合に、確実にすることができる。銀行の方が顧客よりもインフラストラクチャに関わる可能性が高いため、セキュリティにおける顧客の関わりは、一般に、パスワード（「キー」）の選択とパスワードの機密を保持することとに限られる。顧客のタスクがキーを記憶するという簡単なことであるが、銀行のタスクはより複雑である。これは、アタックが通信に介入して通信を安全でないものにする機会が多くあるためである。リスクもまた、顧客よりも銀行の方がずっと大きい。顧客のセキュリティが破られ、アタックが顧客のパスワードを取得した場合、アタックの取り分は通常、1人の顧客の銀行預金口座で入手可能な資金に制限される。顧客が処理中に権限の無いアクティビティに気が付いた場合、その取り分は更に制限される。しかしながら、銀行のセキュリティが危険に晒されている場合、アタックの取り分は制限されず、かつ人目を引かない。このため、銀行は、安全システムを有することに非常に関心を持っている。

【0012】公開キー暗号化が使用される場合、一対のキーが生成され、そのうちの一方が秘密キーであり、他方が公開キーである。いずれの場合も、安全な端末は秘密キーを有している。アタックは、それら秘密キーを取得することができる場合、安全な端末間を行き来するメッセージ・トラフィック上で盗聴することができ、そのトラフィックをインタセプトすることさえできる場合がある。また、場合によっては、秘密キーを知っているアタックが、安全な端末を宛先とするメッセージを変更し、安全な端末によって送信されているメッセージを変更するために十分な知識を有している場合がある。それによって、アタックは、検出されることなく、以降のメッセージ・トラフィックを変更し続けることができる。かかる危険性は、アタックが「キー変更」コマンドと新たな秘密キーとを含むメッセージをインタセプトすると、秘密キーが変更された後でも継続する。

【0013】アクセスが続けられることにより、危険に晒された端末は危険に晒された端末であり続ける。逆に、保護された端末は、通常、適切に設計されている場合、安全な端末であり続けることができる。安全なシステムは、一旦危険に晒されると、安全なシステムと見なすことができない。従って、安全なシステムは、システムの最初のインストールを含む各インプリメンテーション段階において、安全であることが必要である。最初のインストールでの困難の1つは、端末が秘密キーの初期セットで開始する必要がある、ということである。秘密キーの初期セットは、新たなキーとキーを変更するという命令とを含む保護されたコマンド・メッセージを端末に送信することにより、遠隔制御で変更することができる。「キー変更」メッセージが送信される前に端末が危険に晒された場合、アタックがメッセージを読出しその

キーのコピーを更新することができるため、それによって危険性が継続する。暗号化システムの上記脆弱性を鑑みると、暗号化デバイスの初期化プロセスは、暗号化デバイスが安全であるように、注意深く設計されなければならない。

【0014】

【発明が解決しようとする課題】デバイス初期化の1つの解決法は、製造中にキーの初期セットをインストールするというものである。この解決法の欠点は、製造業者が各デバイスの初期キーを追跡し続けなければならないということ、及び、端末の購入者が、その情報を安全にしておくために、製造業者に頼らなければならないということである。初期キーが明白にロードされている場合、プロセスを監視している人は誰でもそのキーを獲得することができ、デバイスのセキュリティを脅かすことができる。あるいは、製造業者は、デバイスがすべて共通の初期キーを有するようにデバイスを製造してもよい。共通の初期キーによって、盗聴者からは安全に最初の一意的キーをロードすることは可能であるが、多くのデバイスに共通のキーのセキュリティは、通常、信用できないものである。

【0015】デバイス初期化の他の方法は、「信用されたエージェント (trusted agent)」方法である。この方法により、暗号化システムは、キー無しに製造され、安全なチャネルによりキーを暗号化システムに入力することによって、暗号化システムの所有者の信用されたエージェントによって初期化される。暗号化システムが安全でないコネクションによって接続されたリモート・ネットワーク (グローバル・インターネット等) 上に配置されている場合、信用されたエージェントは、初期化キーを入力するために暗号化システムのロケーションに移動しなければならない。一般に、エージェントの従業員すべてを必ずしも完全に信用できるものでないため、初期化キーは、エージェントの2人の信用された従業員間に分割される。彼らは、初期化キーのそれぞれの部分を入力するために、暗号化システムのロケーションに各々移動する。当然のことながら、これは費用がかかりかつ時間がかかる。更に、キー入力のためのキーボード等の専用ハードウェアが使用される場合、その分のコストがデバイスに付加され、キーのロードの自動化が妨げられる。

【0016】信用されたエージェントによる方法は、目下、初期キーを新たなATM (自動預金払機) 及びPOS端末 (本明細書では包括的に「端末」と言う) にロードするために使用されている。DESキー部分の二重管理を提供する少なくとも2人のセキュリティ人員は、キー・ロード・デバイスから端末への実際のキーのロードを監視する。一般的なネットワークがかかる端末を何万も有している場合が多いため、このキー・ロード・プロセスは、特にデビットPOS端末の場合に、非常に負

担となる。

【0017】リモート・ロケーションへの移動を避けるために、キー貯蔵所 (deposit) を使用することができる。キー貯蔵所は、すべての暗号化システムが製造後に導かれる安全なロケーションである。このキー貯蔵所において、初期化キーが安全なチャネルを介して暗号化システムにロードされ、その後、暗号化システムは使用される場所に移送される。この方法は、実際の取引では物理的なキー貯蔵所の保持を継続しなければならない、いくつかの余分の移送ステップが必要であるため、コストがいくらか低減するにも関わらず、実質的に別の費用がかかる。

【0018】

【課題を解決するための手段】本発明の1つの実施の形態による暗号化システムにおいて、内部機密を生成するセキュア・セクションを有するデバイスが製造される。内部機密の非可逆性暗号化変換が行われ、非可逆性暗号化変換及びデバイスの一意的識別子を含む証明書 (certificate) に対し、製造業者のキーを用いて署名がなされる。デバイス及び証明書は、ネットワーク・オペレータに提供される。そのオペレータの制御の下、初期化プロセスが実行されることにより、2つのデバイス間の安全な通信のために、オペレータの制御の下で、2つのデバイス間に安全なチャネルがセットアップされる。各デバイス内に保持される内部機密及び証明書により、それらデバイスは互いを認証することができ、それらデバイスがオペレータの機密によって予めプログラミングされている必要なく、安全でないチャネルを介する場合であっても、安全に通信することができる。それらデバイスは、互いを認証することができ、安全でないチャネル全体に互って共有機密を作成することができる。

【0019】

【発明の実施の形態】本発明は、この開示を読めば明らかとなるように、多くのアプリケーションを有している。本発明によるセキュリティ・モジュールの実施の形態の説明においては、可能な変形例を例示的に説明している。更に、この説明において、セキュリティ・モジュールの特定のアプリケーションが、一例として繰返し用いられている。当業者には、他の適用法及び変形例が明らかとなる。そのため、本発明は、実施例のように狭く解釈されるべきではなく、添付の特許請求の範囲に従って解釈されるべきである。

【0020】本システムの説明において繰返し使用されている1つの特定のアプリケーションは、銀行により、その銀行とその顧客との間のメッセージを制御するためにセキュリティ・モジュールを使用することである。銀行は、その資金及び顧客を保護するものであり、資金振替メッセージ及び他の通信が内密で確実であり完全であることを保証すべきである。預金者の資金の強固な保管

者であるために、銀行は、製造業者、銀行の顧客、又は銀行の従業員を完全に信用している訳ではなく、これらが、メッセージ・トラフィック上で盗聴するか、あるいは、内密のメッセージを盗出すようトラフィックを変更するため干渉するか、又はインタセプトする者がまったく権限の無い預金口座から資金が転送されるようにするよう、改竄することが全く無いとは考えていない。

【0021】図1は、銀行又は他のセキュリティに関心があるエンティティによって使用することができるコンピュータ・システム10の一例を示している。システム10において、ネットワーク12上に種々のデバイスが相互接続されている。本明細書において、「製造業者」は、デバイスを作製するエンティティか、又はそのデバイスの製造業者と利害関係を持って提携しているエージェント又は他のエンティティを説明するために使用される。「オペレータ」は、デバイス又はそのエージェントを使用することから利益を得るエンティティ、例えば、オペレータがそのオペレータのデータを送信するためにネットワーク12上にセットアップした、安全なネットワークに、インストールするためにデバイスを購入した購入者を説明するために使用される。本発明において、製造業者とオペレータとは別個のエンティティである必要はまったく無いが、セキュリティの目的で、オペレータの関心は、オペレータが必ずしも製造業者を信用していないということであると想定する。

【0022】ネットワーク12は、信頼性の無いネットワークであるが、本発明は、信頼性の無いネットワークの使用に限定されるものではない。使用可能なネットワークの一例は、ネットワークのうち、一般に「インターネット」として知られるグローバル・インターネットワークである。インターネットは、ほとんど設計により、パケットのルーティングが概して制御されておらず、パケットが、送信側にも受信側にも未知でありかつ制御されない多くの異なるコンピュータ・システムを通してルーティングすることができるため、必ずしも安全ではない。上記ルーティングにより、ルーティング・コンポーネントにアクセスするアタックは、データを盗聴することも変更することも可能である。

【0023】ネットワーク12に接続されている図1に示すデバイスとして、端末14及び安全キー及びデータマネージャ（SKDM）16が示されており、それらの動作は後に詳述する。説明の目的のために、権限の無いすなわち非認可端末14'及び非認可SKDM16'がネットワーク12に接続されている。かかる非認可デバイスはネットワーク12に容易に接続可能であるが、後述するように、認可された端末14及びSKDM16のアーキテクチャ及びコンポーネントにより、非認可デバイス14'、16'は、認可されたデバイスと適切に相互動作が不可能である。

【0024】図2は、端末14の1つの実施の形態をよ

り詳細に示している。図2は端末14のブロック図であるが、SKDM16を同様に構成することも可能である。端末14は、入力／出力（I/O）セクション20と、端末専用ロジック・ブロック22と、セキュリティ・モジュール（SM）24とを備えている。一般的なセットアップでは、端末のオペレータは、端末を製造業者から購入し、オペレータが、自分に特有の目的で使用するために、ネットワーク12上にそれらをインストールする。

【0025】セキュリティ・モジュール24は、セキュア・セクション（SS）26と非セキュア（非保護）・セクション28とを備えている。適切に設計されたセキュア・セクションは、改変不可能すなわち改竄不可能（tamper-resistant）境界等、適切に設計されたセキュア・セクションに共通するいくつかの特性を有している。改変不可能境界により、アタックが、配線の切断又はメモリの消去等の、少なくとも明確な破壊の証拠を残すことなく、セキュア・セクションの内部要素に到達することは困難となっている。他の特性は、セキュア・セクションが、侵入が完了してアタックが機密へのアクセスを取得する前に、侵入が進行中であり機密を消去又は破壊している時にそれを検出する改変検出機構を有していることである。更に、適切に設計されたセキュア・セクションは、セキュア・セクションが改変不可能境界内で保護されたいかなる機密をも解放するような信号、データ入力、又はコマンドが存在しないため、論理的に安全である。

【0026】非セキュア・セクション28は、SS26と端末14の残りの部分との間のI/Oインタフェース等、セキュリティ・モジュール24の動作をサポートするロジック及びデータを含み、該ロジック及びデータは、が安全が維持される必要のないものである。SS26には、機密データ要素も非機密データ要素も格納することができるが、メモリが読出されないように保護する必要がある別のロジックが機密データ要素のみを保護する必要があるため、それらを別々に保持していることが好ましい。

【0027】図3は、SS26のより詳細なブロック図である。SS26は、セクションI/O30と、プロセス・ロジック32（ゲート又はマイクロプロセッサ等）と、記憶装置34と、乱数発生器（RNG）36と、指数演算器38とを有している。記憶装置34に記憶されるデータの詳細は、SS26によって実行される種々のプロセスに関連して後述する。暗号化システムの設計において周知であるように、セキュリティ・オペレーションによっては、乱数と指数値とによるものがあるため、アタックは、乱数発生器（RNG）36によって発生する乱数と指数演算器38が実行する指数法とを制御又は観測することにより、システムのセキュリティを破ることができる。従って、乱数発生器（RNG）36及び指

数演算器38は、好ましくはSS26の改変不可能境界内で保護されている。

【0028】ここで、端末を動作させるプロセスを説明する。端末専用ロジック・ブロック22の初期化は、端末の特定の使用法によって決まるものであり、それは、ここでの説明の範囲外であるため、焦点をセキュア・セクション26の初期化に置く。SS26の初期化を2つの部分で説明する。第1の部分は、SS26の製造業者によって行われる動作を詳述し、第2の部分は、SS26のオペレータによるか又はオペレータのために行われる動作を詳述する。図4にはSS製造プロセスが示されている。示されている製造環境100において、製造初期化ファシリティ(MIF)110は、製造ワークステーション(MWS)112を備えている。MSW112は、MIF110内で安全な製造インストール・セキュリティ・モジュール(MISM)114に結合されている。また、MIF110は、MIF110によって初期化されるセキュリティ・モジュールに関するデータを含む製造データベース116を有している。

【0029】ターゲットであるSS126を有するターゲットSM124が、リンク120を介してMIF110に連結されている。以下に述べるプロセスにおいて、ターゲットSM124は、初期化中のSMである。リンク120は、データ改変からのみ安全である必要がある。すなわち、ターゲットSS126からMWS112に送信されるデータは、変更されずにMWS112によって受信され、MWS112からターゲットSS126に送信されるデータは、ターゲットSS126によって受信される。また、リンク120は、盗聴から安全であるようにすることが可能であるが、それは、ターゲットSS126の初期化の全体的な完全性を維持するためには必要ではない。

【0030】初期化プロセスに先立って、ターゲットSS126を包括的なもの(generic)、すなわち、個々のターゲットSS126は同一であるとして行うことができる。ターゲットSS126は、MIF110によって初期化プロセスが実行されることによって、包括的でなくなる。1つのかかる初期化プロセスの詳細は、図4において順序付けられたステップを示す○で囲まれた数字によって示されている。対応する数字は、下記の本文において、対応するステップの近傍に挿入されている。

【0031】最初に、MIFは、ターゲットSSに対して通し番号SSIDを生成し、SSIDをターゲットSSに渡す(ステップ1)。ターゲットSSは、記憶装置34にSSIDを記憶し(ステップ2)、公開キー・ペアKSSを生成して(ステップ3)記憶装置34に公開キー・ペアを格納する。KSSは、秘密部分KPVSSと公開部分KPBSSとを有している。KSSの生成は、SSIDの受信、MIFからのコマンドの受信又は

他の適切なトリガによってトリガすることができる。ターゲットSSは、KSSを生成すると、公開部分(KPBSS)をMWSに送信する(ステップ4)。ターゲットSSがインストールされるシステムの全体のセキュリティの一部として、秘密部分KPVSSは、ターゲットSS内に残り、ターゲットSSの外側と通信する必要がなくなる。

【0032】MSWはKPBSS及びSSIDをMISMに提供し、MISMは製造業者証明書MCertを生成する。製造業者証明書は、KPBSSを含んでおり、MIF秘密署名キーKPVSIGMによって署名され、MISM内に保持される(ステップ6)。MISMは、MIFによって任意のSSが初期化される前に、MIF署名キー・ペア(KPVSIGM, KPB SIGM)によって初期化される。また、製造業者証明書は、SSID、証明書バージョン番号、デバイス許可(ターゲットSSに対する)及びアルゴリズム・パラメータ(ターゲットSSによって使用される)を含むことができ、それらの使用法は以下に説明されている。製造業者証明書は、MISMからターゲットSSに渡され、ターゲットSS内において、MIFの公開署名キーKPB SIGMと共に記憶される(ステップ7)。KPB SIGMもまた、ターゲットSS内に記憶されるものである。また、MIFは、SSID及びMCertのコピーを含む検査証明書130を生成する(ステップ8)。

【0033】この時点で、ターゲットSSは、正式に製造されたデバイスとなる。それは、特定の識別子(SSID)を有しているため、非包括的ではあるが、一般にターゲットSSを使用する最終的なオペレータに特有なものではない。しかしながら、ターゲットSSは、各オペレータに対して異なるMIF署名キー・ペア(KPV SIGM, KPB SIGM)を使用することにより、オペレータに特有なものとして行うことができる。いずれにしても、ターゲットSSは、好ましくはこの時点でいかなるオペレータ機密をも含んでいない。以下に、オペレータがセットアップしたネットワークに対して、デバイスを特有なものにコンフィギュレーションするための初期化プロセスを説明する。

【0034】ターゲットSSがオペレータに与えられる時、そのオペレータには、ターゲットSSに属する検査証明書130が与えられる。検査証明書は、それ自体保護された証明書である必要はないが、好ましくは、オペレータに対して個別に密かに与えられる。検査証明書により、オペレータは、密かに引き渡されたターゲットSSが、所定の一意的な識別子(SSID)を有しておりかつ製造業者によって適切に初期化されている、ということを確認することができる。そして、オペレータは、ターゲットSSをSM24内にSSとしてインストールすることができる。あるいは、製造業者は、SM24内にすでにインストールされているSSを提供するか、又

は、端末14又はSKDM16にすでにインストールされているSSをSM24に提供することも可能である。

【0035】オペレータは、ターゲットSSを取得すると、該ターゲットSSをネットワーク12（安全でない可能性が高い）に接続する。一般に、オペレータは、ネットワーク12上で1つ又は複数のSKDMを実行し、SSによってとられる第1の動作は、キー・ロード・キー及びキー変更キー等の、オペレータ機密をSKDMからSSにローディングすることである。オペレータのセキュリティに対する関心の1つは、SKDMが権限のない端末すなわち非認可端末14'にキーをローディングしないこと、及び、SSが非認可SKDM16'からコマンド及びキーを受入れないということである。従って、SS及びSKDMは、オペレータ機密を脅かすために使用することができるいかなるオペレータ機密又はデータが転送される前に、互いを認証しなければならない。

【0036】オペレータ初期化プロセス（初期化プロセスの第2の部分）において、SS及びSKDM（又は、更には言えば2つのSS）は、信頼性の無いチャネルによって接続される。なお、このプロセスは、安全でないネットワークに接続されたデバイスによって行うことができ、その場合、データは観測も変更も可能な状態である。このプロセスは、デバイスにおいてオペレータ機密のインストールを先に行うことなく実行することができる。

【0037】オペレータによって操作される2つのデバイス間で使用可能な特定の相互認証プロセスの一例が、図5のフローチャートに示されている。図5に示したプロセスの変形例は、この説明から当業者には明らかとなるであろう。図5のフローチャートのステップは、ステップS1から始まる番号が付されており、それら番号は、括弧を用いて、以下の本文に挿入されている。これらステップは、番号が付された順序で実行されるが、当業者にとっては、この説明から、番号の大きい1つのステップに対しそれより番号の小さいステップがその番号の大きいステップの前に行われる必要がない場合、ステップの順序を変更することができることは、明らかであろう。

【0038】図5に示すプロセスは、2つのデバイス、すなわちデバイスA及びデバイスBを相互に認証し、その結果、デバイスA及びデバイスBのみに既知の共有機密を生成する。当然のことながら、アタッカの計算能力又は時間が十分ある場合、共有機密はアタッカによって取得が可能であるため、システムは、計算能力又は時間が労力に見合わずにアタックを行うには高過ぎるように設計されていなければならない。後述するプロセスの1つの利点は、共有機密の生成が相互認証プロセスと絡み合っている、ということである。プロセスの他の利点は、認証センタ及び2つのデバイス間の認証チェーンを

必要とすることなく、相互認証プロセスを行うことができる、ということである。デバイスAは、端末14でもSKDM16であってもよい（より正確には、それらデバイスのうちの1つのSM24）。また、デバイスBは、端末14であってもSKDM16であってもよい。例えば、デバイスA、Bは、端末とSKDMとであってもよく、又は両デバイスとも端末であってもよい。

【0039】プロセスは、デバイスAが認証のためにキー折衝キー（KNK）のペア（KPVA1, KPBA1）を生成することから開始する（ステップS1）。上述した製造プロセスに続いて、デバイスAは、一意的すなわちデバイスAに特定の識別子（図5においてIDAとラベル付けされている）、内部機密KPVA及びデバイスAの製造業者証明書（MCertA）等、いくつかのデータ要素を含んでいる。なお、内部機密KPVAは、デバイスAのセキュア・セクション内で作成されており、セキュア・セクション外部、及び製造業者に対してさえも開示される必要は無い。デバイスAは、2つのメッセージM1及びM2を作成し、それらメッセージをデバイスBに送信する。メッセージM1は、KPVAによって署名されたIDA及びKPBA1を含んでいる。

【0040】デバイスBは、M1及びM2を受信すると、KPBSIGM、すなわち製造業者公開署名キーを用いて、M2の検査すなわち認証を行う（ステップS2）。M2が有効でない場合、デバイスBはプロセスを停止して、デバイスAが権限の無いデバイスすなわち非認可デバイスであると推定する。有効である場合、デバイスBは、M2からKPBAを抽出する（ステップS3）。KPBAはキーの公開部分であり、KPVAはキーの秘密部分である。先に説明したように、公開部分は、製造業者証明書に含まれていたものである。この時点で、デバイスBは、製造業者が証明したことにより、KPBAが実際にはキーの公開部分であると確認する。

【0041】ステップS4において、デバイスBは、KPBAを用いてM1を照合する。M1が有効でない場合、デバイスBはプロセスを停止し、デバイスAが非認可デバイスであると推定する。M1が有効である場合、デバイスBは、M1からKPBA1を抽出する（ステップS5）。この時点で、デバイスBは、デバイスAを認証したことになる。デバイスBを認証するデバイスAのプロセスには、ステップS6～S11が含まれる。なお、ステップS1～S5は、ステップS6～S11に対して特定の順序で発生する必要はない。しかしながら、M3及びM4をデバイスBからデバイスAに渡される機密とすることが望ましい場合、デバイスBは、少なくともデバイスBにおいて共有機密を生成するために十分なステップを実行することができる。

【0042】ステップS6において、デバイスBは、認証のために自身のキー・ペア（KPBVB1, KPBB1）を生成する。デバイスAと同様に、正式に製造され

たデバイスBは、いくつかのデータ要素を有している。デバイスBにおけるそれらデータ要素には、一意的な識別子（図5のID_B）、内部機密K_{PVB}及びデバイスBの製造業者証明書（MCert_B）が含まれる。内部機密K_{PVB}は、デバイスBのセキュア・セクション内で作成されており、セキュア・セクション外部に開示される必要はない。K_{PVB1}は、後のステップにおいて、共有機密を生成するために用いられる。デバイスBは、2つのメッセージ、すなわちM₃、M₄を作成し、それらメッセージをデバイスAに送信する（ステップS₇）。メッセージM₃は、K_{PVB}によって署名されたID_B及びK_{PBB1}を含んでいる。デバイスAは、M₃及びM₄を受信すると、K_{PBS1GM}、すなわち製造業者公開署名キーを用い、てM₄を照合する（ステップS₈）。M₄が有効でない場合、デバイスAはプロセスを停止し、デバイスBが権限の無いデバイスすなわち非認可デバイスであると推定する。有効である場合、デバイスAは、M₄からK_{PBB}を抽出する。K_{PBB}は、キーの公開部分であり、K_{PVB}はキーの秘密部分であって、MCert_Bに含まれている。この時点で、デバイスAは、製造業者が証明したことにより、K_{PBB}が実際にはキーの公開部分であると確認する。

【0043】ステップS₁₀において、デバイスAはK_{PBB}を用いてM₃を照合する。M₃が有効でない場合、デバイスAはプロセスを停止して、デバイスBが権限の無いデバイスすなわち非認可デバイスであると推定する。M₃が有効である場合、デバイスAは、M₃からK_{PBB1}を抽出する（ステップ11）。この時点で、デバイスAは、デバイスBを認証（承認）しており、デバイスBはデバイスAを認証している。更に、この時点で、デバイスAは、K_{PVA1}及びK_{PBB1}を有しており、デバイスBは、K_{PVB1}及びK_{PBA1}を有している。これらの2つの値の各々を用いて、各デバイスは、共有機密を生成することができる。各デバイスが共有機密を生成すると、2つのデバイスは、共有機密（S_{12A}、S_{12B}）を使用することによって、互いの間で機密に通信することができる。共有機密を生成するための方法を後述するが、他の方法を用いて共有機密を生成することも可能である。システムによっては、K_{PBS1GM}のセキュリティによらずに共有機密を生成することが好ましい場合もあり、それによってオペレータのシステムはK_{PBS1GM}が危険に晒された後に危険に晒されることはない。

【0044】共有機密を生成する1つの方法は、Diffie-Hellman（DH）交換である。DH交換は、機密であっても無くてもよい2つの変数、 α 及び n を使用するものであり、ただし $\alpha < n$ である。デバイスAは、 $K_{PBA1} = \alpha K_{PVA1} \bmod (n)$ であるキー・ペアを生成し、デバイスBは、 $K_{PBB1} = \alpha K_{PVB1} \bmod (n)$ であるキー・ペアを生成する。デバイスA

は、M₃からK_{PBB1}を抽出すると、 $Y_A = K_{PBB1} K_{PVA1} \bmod (n)$ を計算することができ、デバイスBは、M₄からK_{PBA1}を抽出すると、 $Y_B = K_{PBA1} K_{PVB1} \bmod (n)$ を計算することができる。

なお、これら値が生成された方法から、以下のように表すことができる。

$$\begin{aligned} Y_A &= K_{PBB1} K_{PVA1} \bmod (n) \\ &= (\alpha K_{PVB1}) K_{PVA1} \bmod (n) \\ &= (\alpha K_{PVA1}) K_{PVB1} \bmod (n) \\ &= K_{PBA1} K_{PVB1} \bmod (n) \\ &= Y_B \end{aligned}$$

従って、 $Y_A = Y_B$ であって個別のアルゴリズムを実行することが困難であるため、デバイスA及びBは共有機密を有する。ある実施の形態において、 n は大きい素数（1024ビットのオーダ）であり、 α は2 q の元を有する有限体の1つの元である（ q は、 $n-1$ 及び α を除算する160ビットの素数）。 $Y = Y_A = Y_B$ が1024ビットのオーダである場合、56ビットDESキー等のキーを Y から作成することができる。共有機密が作成されると、該共通機密を種々の使用法で用いることができる。

【0045】図3は、記憶装置34に記憶されたデータ値の詳細を示している。より詳細には、記憶装置34は、以下に示す要素に対する記憶領域を含む。

バージョン番号 端末がセキュア・チャネル及び／又は交換キーをセットアップするために使用するプロトコルのバージョン

SSID 特定の端末／ターゲットSSに一意の、製造業者が割当てた値

許可フラグ いかなる作用が可能であることを示すフラグ

キーロードタイプ 初期自動キー・ロード・プロセスにおいて発生するキー・ロードのタイプ（例：キー交換キー、一時スーパ・キー、端末キー・ロード・キー

KSS 端末用のキー・ペア（K_{PVSS}、K_{PBSS}）

K_{PBS1GM} 製造業者の署名キーの公開部分

MCert 製造業者証明書：ターゲットSSのオペレータに特有の製造業者キーを用いたKSSの署名（署名されたデータには、バージョン番号、SSID、許可フラグ及びKSSが含まれる）

CD チェック数字

【0046】MCertに許可フラグが含まれている場合、端末は、一旦MIFによって割当てられるとその許可を変更することができない。許可フラグは、オペレータによって要求されると、端末が実行することができる。例えば、許可フラグは、以下のものを示すことができる。

a. MFKを複数のセキュリティ・モジュール間で共有

することができるか。

b. 端末が他のMFKをロードすることが許可されているか。

c. 端末にアプリケーション・プログラムをローディングする。

d. 端末がキー交換キー（KEK）をローディングすることが許可されているか。

e. 端末が特定の端末キーをローディングすることが許可されているか。

f. DSA署名が照合されるべきか。

【0047】端末14の特定の目的は、この開示の主要な面ではないが、端末14は、購入者情報を収集するか又は電子取引をもたらすために使用されるポイント・オブ・セール（POS）端末か、自動預金支払機（「ATM」）か、スマート・カード・リーダ等であってもよい。場合によっては、端末14は、ある特定の目的に対するセキュリティ・モジュール24、及び端末製造業者又は後に付加された別個のセキュリティ・モジュールの製造業者によって製造されたセキュリティ・モジュール無しに、製造されてもよい。例えば、ATMを、セキュリティ・モジュール無しに、ATMに特有のロジックで製造することができる。そして、ATMに特有でないセキュリティ・モジュールをATMに付加することが可能である。

【0048】他の例では、端末はパーソナル・コンピュータであり、セキュリティ・モジュールはそのパーソナル・コンピュータにインストールされたPCバス・カードである。パーソナル・コンピュータとセキュリティ・モジュールとが1つの会社によって製造されている場合、パーソナル・コンピュータは、ブレインストールされたセキュリティ・モジュールを備えて出荷することができる。初期化が製造時に行われることにより、パーソナル・コンピュータは、オペレータに関連して特有に製造される必要はなく、それにより、オペレータにパーソナル・コンピュータを提供するプロセスが簡略化される。

【0049】大規模機構組織は、何万台ものパーソナル・コンピュータを使用する可能性があり、それらにはすべて、パーソナル・コンピュータが安全でないネットワーク上で安全に相互通信することができるように、セキュリティ・モジュールがインストールされている必要がある。上述したようなセキュリティ・モジュールが無い場合、組織は、マスタ・ファイル・キー等の、機構組織の機密を含む、特に組織に対して特別に事前環境設定されたセキュリティ・モジュールを有する必要があるか、あるいは、パーソナル・コンピュータのインストールの時点まで、それら組織の機密を安全に移送するためのインフラストラクチャを必要とする。しかしながら、上述したセキュリティモジュールを有することにより、機構組織は、中央で、それ自身のキーを管理し、好まし

くは組織内のパーソナル・コンピュータのエンド・ユーザに透過的な方法で、それらを信頼性の無いチャネル上で分配させることができる。エンド・ユーザは、初期化ルーチンを実行する必要があるだけであり、その後、セキュリティ・モジュールを起動して、図5に示す相互認証プロセスを実行し、キー・サーバから動作のためのキーを取得することができる。

【0050】図6は、デバイスをオペレータ特有にするために汎用デバイスにキーをローディングするための、信頼性の無いネットワークに接続される可能性のあるキー・サーバ150を示している。1つの実現例において、キー・サーバ150は、安全な物理的環境にあるウィンドウズ（登録商標）NTサーバである。キー・サーバ150は、サーバ・ソフトウェア152、端末データベース154、監査ログ156、及びネットワーク1/O158を備えている。ネットワーク1/O158は、キー・サーバ150を信頼性の無いネットワーク12に接続すると共に、保護されたコネクションを介して、キー・サーバ150をセキュリティ制御端末（SCT）160に接続する。図示されているように、SCT160は、保護されたすなわち安全な1/O162を介して、ユーザに対するインタフェースを有している。

【0051】端末データベース154は、セキュア・セクションの各々のMCertと同様に、オペレータが使用する各セキュア・セクションに対する通し番号（SSID）のリストを保持している。オペレータは、更に多くの端末をオンライン化する時、新たな端末各々に対し、端末データベース154にSSID及びMCertを付加することができる。

【0052】キー・サーバ150内における暗号化動作は、キー・サーバ150内のセキュリティ・モジュール24'によって実行される。キー・サーバ150が複数のサブネットワークを管理している場合、キー・サーバ150内で、複数のセキュリティ・モジュール24'が使用されてもよい。セキュリティ・モジュール24'を上述したセキュリティ・モジュール24を同じのものとすることができるが、キー・サーバによっては、自動キー生成機能が必要とされないものもある。その代りに、キー・サーバの初期キーが安全なコネクションに亙ってマニュアルでロードされる。安全なコネクションの1つは、SCT160によって提供され、安全な方法でマスタ・ファイル・キー（MFK）をローディングし、セキュア・セクションからデータを読み出すことができるものである。

【0053】上述した方法で、データ完全性もデータ機密性も保証されていない安全でない非セキュア・チャネルを介して、1つ端末と1つのキー・サーバ、又は2つの端末同士を安全に接続させることができ、安全にメッセージを通信し、他のパーティの会話に対する権限を照合することができる。これにより、2つの端末はそれら

の間でメッセージを通信するか、共有機密をセットアップするか、又は非セキュア・チャンネルによりキーの安全なローディングを調整することが可能になる。例えば、図5に示すプロセスが完了すると、キー・サーバは、キー又は「キー変更」コマンドの新たなセットをSSに安全に送信することができ、SSは、キー・サーバがキーの変更の前に要求されたものであることを照合することができる。

【0054】誰かが検出されずに許可されていないデバイスをネットワークに挿入し、それをキー・サーバによって照合させることを防止するために、キー・サーバはキー・サーバがそれを用いて実行した端末の監査ログ156を保持する。監査ログ156の記録には、端末の製造業者製造ID（SSID）と、通し記録番号とが含まれる。通し記録番号は、監査ログ156からの記録の削除を明らかにする。変更を防止するために、記録は署名されていることが可能である。ここでは、キーの初期セットをロードするために安全なチャンネルを必要とすることなく、1つ又は複数のキーの初期セットをロードするシステムが説明された。このシステムにより、安全でないネットワークを介してセキュア・セクションを安全に初期化し認証することができる。

【0055】上述した説明は、例示的なものであって限

定的なものではない。当業者には、この開示を検討することにより本発明の多くの変形例が明らかとなろう。従って、本発明の範囲は上記説明に関して判断されるべきではなく、添付の特許請求の範囲とそれらの同等物の全範囲とに関して判断されるべきである。

【図面の簡単な説明】

【図1】ネットワークに相互接続された保護されたデバイスのブロック図である。

【図2】セキュア・セクションを有するセキュリティ・モジュールを含む、図1の保護されたデバイスの詳細なブロック図である。

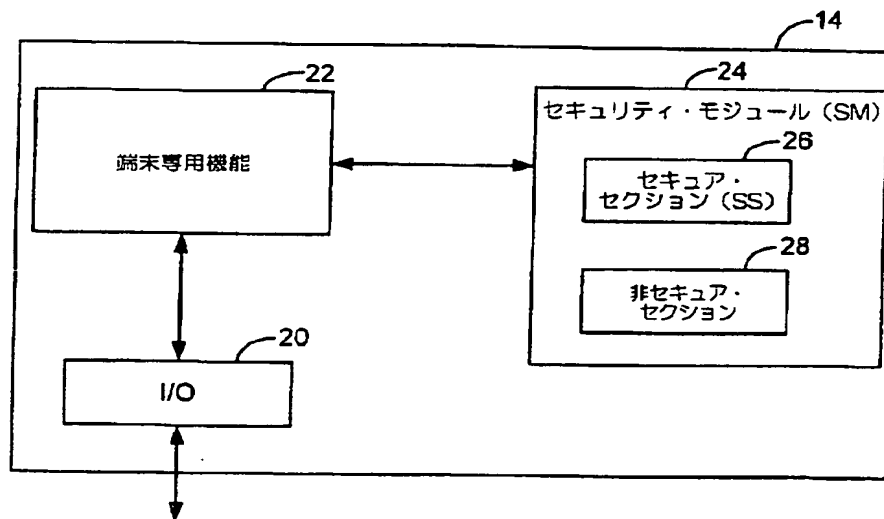
【図3】図2のセキュア・セクションの詳細なブロック図である。

【図4】図1～図3に示されているデバイスに対する製造初期化プロセスを示す製造初期化ファシリティのブロック図である。

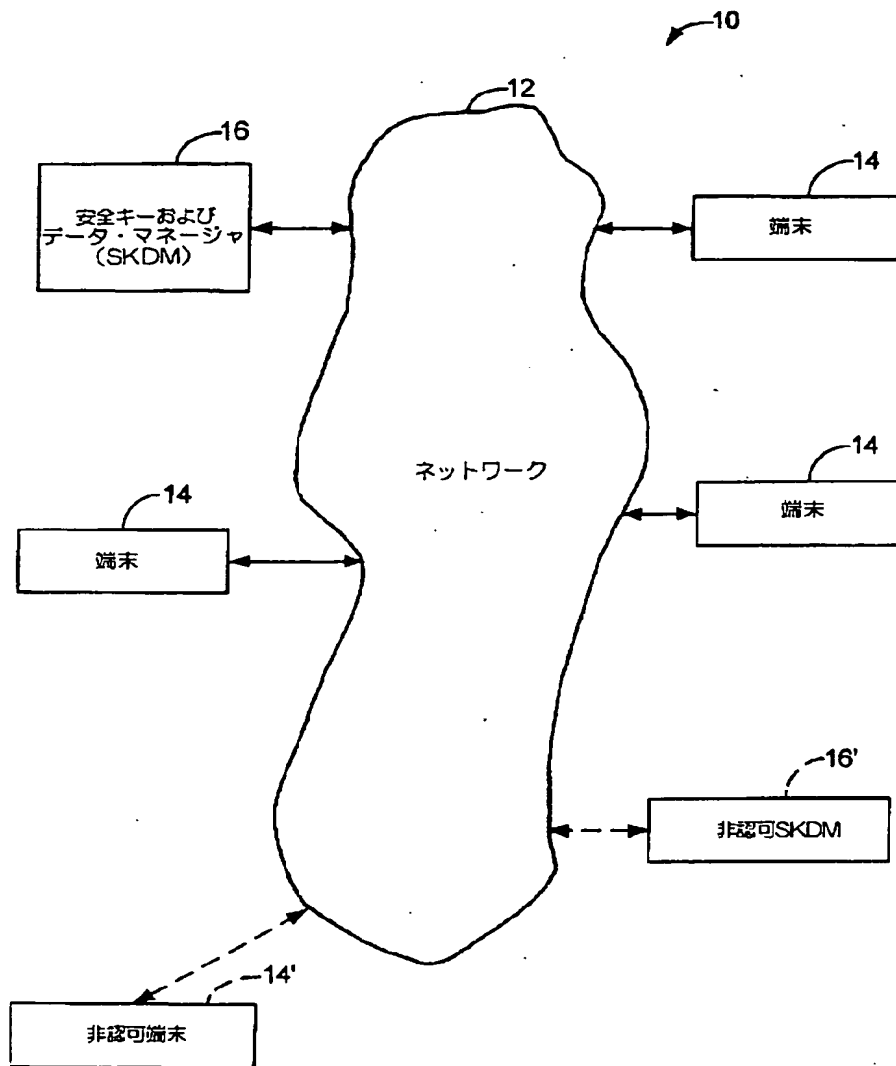
【図5】信頼性の無いチャンネルによって接続された2つのデバイス間に発生する自動キー初期化、相互認証、及び共有機密生成のプロセスのフローチャートである。

【図6】自動キープロセスを用いてネットワークに結合されたデバイスを初期化するために、図1に示すネットワークによって使用されるキー・サーバのブロック図である。

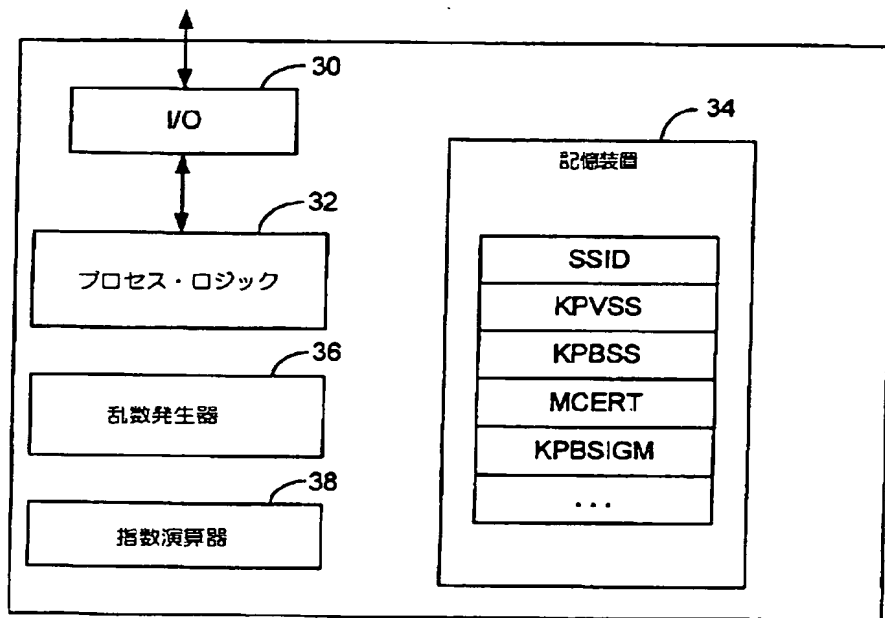
【図2】



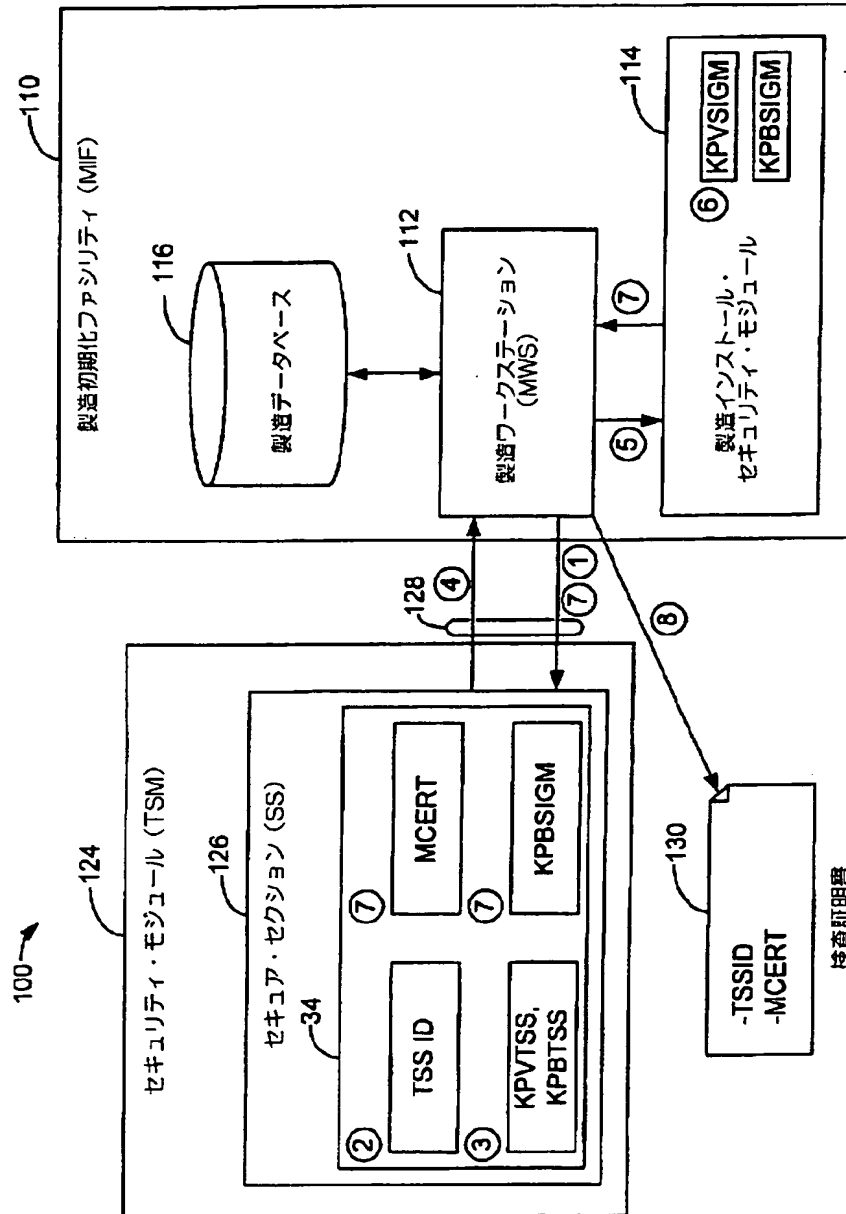
【図1】



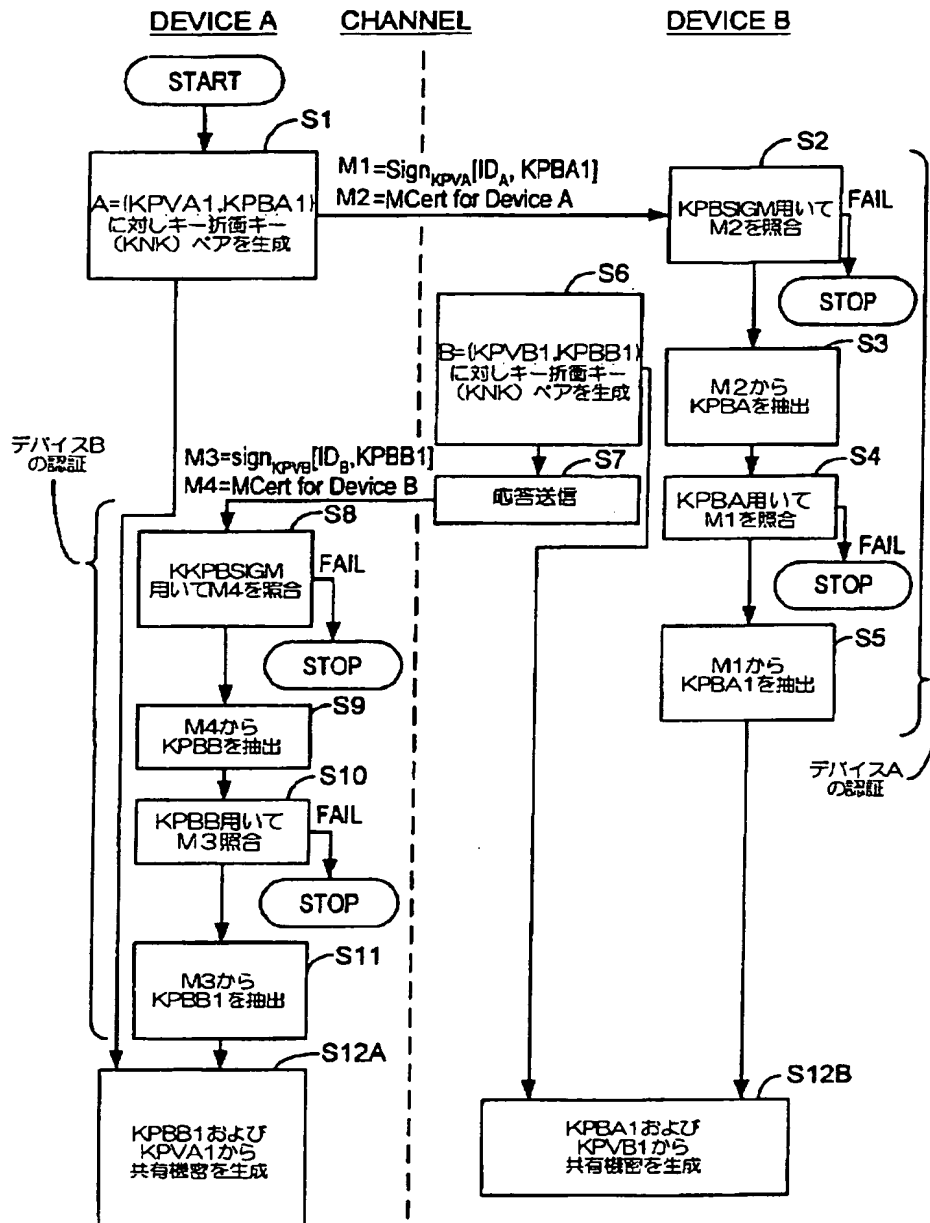
【図3】



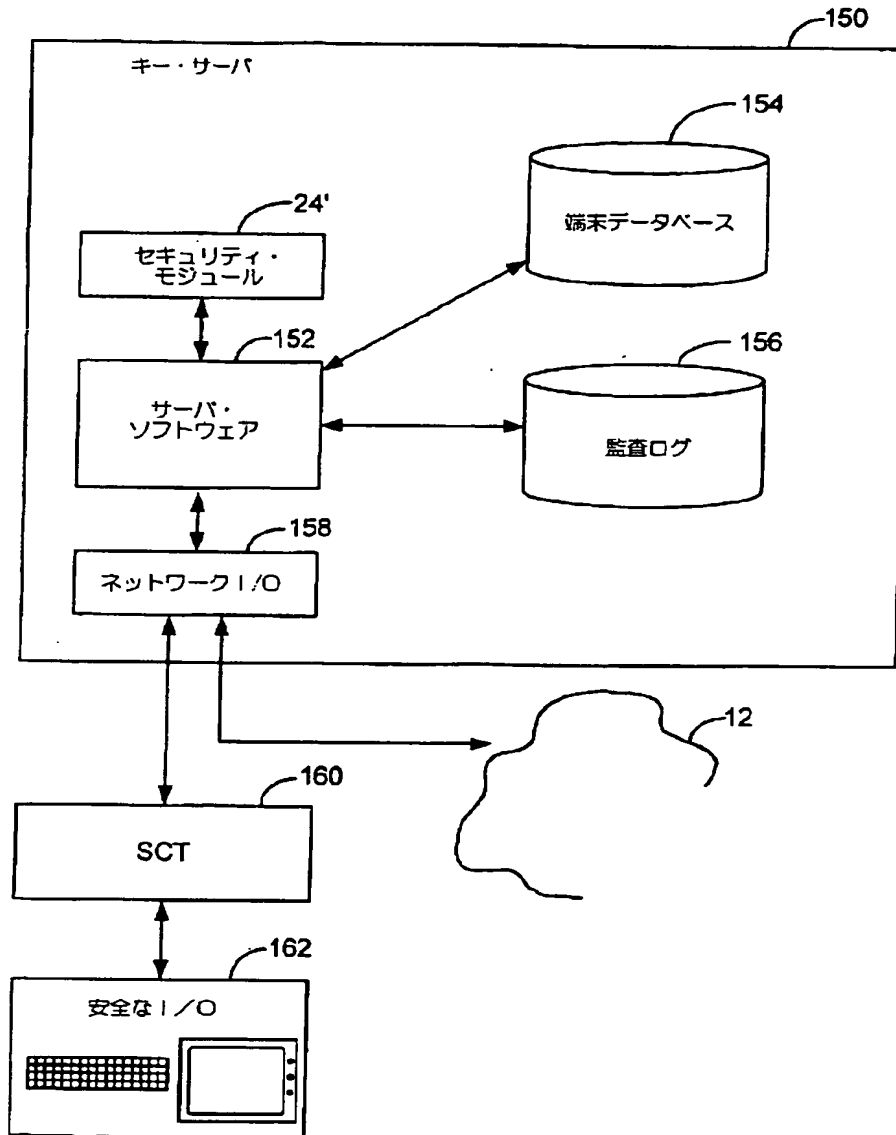
【図4】



【図5】



【図6】



フロントページの続き

(71) 出願人 591030868
20555 State Highway
249, Houston, Texas
77070, United States of America

(72) 発明者 マイケル・マッケイ
アメリカ合衆国カリフォルニア州、ベンロ
モンド、グレンアーバー・ロード 8727

(72) 発明者 スーザン・ラングフォード
アメリカ合衆国カリフォルニア州、サニー
ヴェイル、ポプラ・アベニュー 1275, ナ
ンバー 101

(72) 発明者 ラリー・ハイネス
アメリカ合衆国カリフォルニア州、サン
タ・クララ、パークビュー・ドライブ
610, ナンバー 105